

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
4. April 2002 (04.04.2002)

PCT

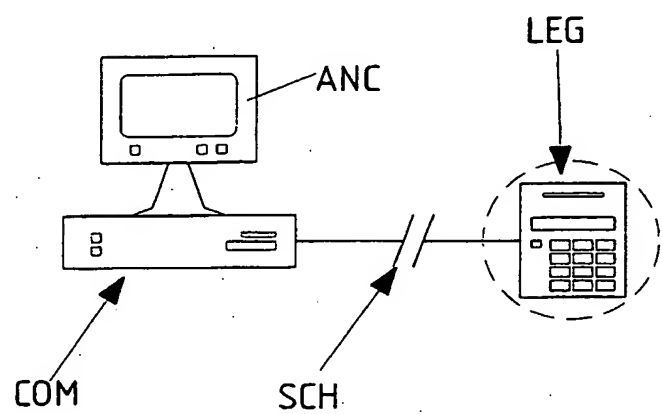
(10) Internationale Veröffentlichungsnummer
WO 02/28005 A2

- | | | |
|---|--|---|
| (51) Internationale Patentklassifikation: | H04L 9/00 | (72) Erfinder: MAHDJOOBAN, Kaveh; R. Zellergasse 47, A-1230 Wien (AT). LEMP, Heinz, Karl; Berzeliusgasse 14/47/4, A-1210 Wien (AT). BÄCKER, Josef; Am Gehsteig 10, A-3442 Langenschönbich (AT). |
| (21) Internationales Aktenzeichen: | PCT/AT01/00299 | |
| (22) Internationales Anmeldedatum: | 24. September 2001 (24.09.2001) | (74) Anwalt: MATSCHNIG, Franz; Siebensterngasse 54, A-1070 Wien (AT). |
| (25) Einreichungssprache: | Deutsch | (81) Bestimmungsstaaten (national): CZ, HU, NO. |
| (26) Veröffentlichungssprache: | Deutsch | (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR). |
| (30) Angaben zur Priorität: | A 1635/2000 27. September 2000 (27.09.2000) AT | |
| (71) Anmelder: SIEMENS AG ÖSTERREICH [AT/AT]; Siemensstrasse 88-92, A-1210 Wien (AT). | | Veröffentlicht: ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts |

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND READER USED TO PRODUCE DIGITAL SIGNATURES

(54) Bezeichnung: VERFAHREN UND LESEGERÄT ZUR ERZEUGUNG DIGITALER SIGNATUREN



(57) Abstract: The invention relates to a method for producing digital signatures for data stored on a data processing device (COM). A reader (LEG) can be connected to the data processing device via an interface (SCH), and serves to read out a signature key from a storage medium to produce a digital signature. The data to be signed are transmitted from the device (COM) via the interface (SCH) to the reader (LEG), where a check sum regarding the transmitted data is produced. The correspondence between the data transmitted to the reader and the data to be signed is verified using specific features of the data. When the data do correspond, a digital signature is produced in the reader using the check sum and the signature key stored on the storage medium. Said signature is transmitted to the data processing device (COM) via the interface (SCH) and the data to be signed are provided with the signature in

the data processing device. The invention further relates to a reader (LEG) for use in the method according to the invention.

WO 02/28005 A2

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Erzeugung digitaler Signaturen für auf einem Datenverarbeitungsgerät (COM) gespeicherte Daten. Über eine Schnittstelle (SCH) ist ein Lesegerät (LEG) an das Datenverarbeitungsgerät anbindbar, mittels welchem von einem Speichermedium ein Signierungsschlüssel zur Erzeugung einer digitalen Signatur auslesbar ist. Die zu signierenden Daten werden über die Schnittstelle (SCH) von dem Gerät (COM) an das Lesegerät (LEG) übermittelt, und in diesem wird eine Prüfsumme über die übertragenen Daten gebildet. Die Übereinstimmung der auf das Lesegerät übertragenen Daten mit den zu signierenden Daten wird an Hand spezifischer Merkmale der Daten überprüft, und bei einem Übereinstimmen der Daten wird in dem Lesegerät aus der Prüfsumme unter Verwendung des auf dem Speichermedium abgespeicherten Signierungsschlüssels eine digitale Signatur erzeugt und über die Schnittstelle (SCH) an das Datenverarbeitungsgerät (COM) übertragen, wo die zu signierenden Daten mit der Signatur versehen werden. Weiters betrifft die Erfindung ein Lesegerät (LEG) zur Verwendung bei dem erfindungsgemässen Verfahren.



Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

VERFAHREN UND LESEGERÄT ZUR ERZEUGUNG DIGITALER SIGNATUREN

Die Erfindung betrifft ein Verfahren zur Erzeugung digitaler Signaturen für Daten, welche auf einem Gerät zur Verarbeitung von Daten oder einem dem Gerät zugeordneten Speicher gespeichert sind, unter Verwendung eines auf einem physikalisch von dem Gerät oder dem Speicher getrennten Speichermedium gespeicherten Signierungsschlüssels, welcher mittels eines an das Gerät über eine Schnittstelle anbindbaren Lesegerätes von dem Speichermedium zur Erzeugung einer digitalen Signatur auslesbar ist.

Weiters betrifft die Erfindung ein Lesegerät für Speichermedien, welches über zumindest eine Schnittstelle mit Geräten zur Datenverarbeitung verbindbar ist, mit einer Leseeinrichtung, zumindest einem Prozessor, zumindest einer Speichereinrichtung, zumindest einer Ausgabe und zumindest einer Eingabe.

Aufgrund ihrer Effizienz, Aktualität und Schnelligkeit gewinnt die elektronische Abwicklung von Kommunikation immer mehr an Bedeutung. Neben allgemeinen Informationen werden über Datennetze auch beispielsweise wichtige Verträge, Vereinbarungen und sogar Register, wie das Grundbuch, künftig elektronisch geführt. Dabei weist natürlich der Sicherheitsaspekt in Hinblick auf Vertraulichkeit und Verbindlichkeit besonders hohe Bedeutung auf.

Bei herkömmlichen Briefen wird die Verbindlichkeit durch die Unterschrift des Verfassers erzeugt. Bei elektronischen Dokumenten ist diese Vorgangsweise allerdings nicht möglich. Das Einscannen der eigenen Unterschrift und das Anhängen oder Einfügen dieser gescannten Unterschrift an das Dokument kann von Unberechtigten auf einfache Weise nachvollzogen und so im Grunde jedes beliebige Dokument mit einer „falschen“ Unterschrift versehen werden.

Eine sichere Lösung für diese Unterschriftsproblematik stellt die digitale Signatur dar, welche durch mathematische Verknüpfung des Textes mit einem persönlichen und geheimen Signaturschlüssel erzeugt wird. Empfänger können diese Signatur mit einem öffentlichen Schlüssel prüfen und dabei nicht nur die Echtheit des Absenders sondern auch die Integrität, also die Unverfälschtheit der übertragenen Daten, feststellen.

Bei Erstellen der digitalen Signatur etwa für ein Dokument laufen komplizierte mathematische Berechnungen ab, die allerdings für den Benutzer nicht erkennbar sind und auf die hier auch nicht näher eingegangen werden soll. Zum Erstellen der Signatur braucht der Benutzer einen privaten Schlüssel. Die Sicherheit der digitalen Unterschrift liegt in der Geheimhaltung dieses Schlüssels sowie in der Schlüssellänge. Aus diesen Gründen ist der Schlüssel zumeist auf einer Chipkarte gespeichert, mit welcher auch der Signiervorgang durchgeführt wird. Außerdem ist beispielsweise nach dem deutschen oder österreichischen Signaturgesetz, welches die rechtliche Grundlage für die Verwendung von digitalen Signaturen liefert, sogar zwingend vorgesehen, dass zur Erzeugung der Signatur eine Chipkarte mit darauf gespeichertem privaten Schlüssel verwendet wird.

Bei einem Signiervorgang von auf einem Computer abgelegten Daten, etwa in einer Datei, ist es notwendig, dem Computer den auf der Karte abgespeicherten Schlüssel zuzuführen. Dies geschieht in der Regel mittels eines Kartenlesegerätes, welche über eine Schnittstelle mit dem Computer verbunden ist.

Damit etwa im Falle eines Verlustes der Signatur-Chipkarte die Signatur eines Benutzers nicht von anderen unberechtigt verwendet werden kann, ist der Karte zumeist ein PIN-Code („Personen-Identifikations-Nummer“) zugeordnet. Durch Eingabe des entsprechenden PIN-Codes über die PC-Tastatur authentifiziert sich der Benutzer als berechtigt, und der Signiervorgang wird von dem Computer durchgeführt, nachdem ihm über das Kartenlesegerät der private Schlüssel übermittelt wurde.

Allerdings bestehen auf diese Weise noch immer Sicherheitslücken, aufgrund derer bei Verwendung eines Computers bzw. bei der Signierung von auf einem Computer gespeicherten Daten keine Sicherheit gegen unbefugte Zugriffe erreicht werden kann. So ist es beispielsweise möglich, den PIN-Code mittels geeigneter Hard- und/oder Software auszulesen, während er von der Computertastatur über den Computer an das Chipkartenlesegerät übertragen wird.

Außerdem besteht natürlich auch die Gefahr, dass der PIN-Code mittels entsprechender Software einfach bereits unmittelbar nach der Eingabe über die Tastatur, ohne dass noch eine Übertragung an das Lesegerät erfolgt ist, ausgelesen wird.

Es ist eine Aufgabe der Erfindung, die erwähnten Sicherheitslücken für Signiervorgänge, bei denen ein Gerät zur Datenverarbeitung, etwa ein Computer, Verwendung findet, bzw. die Sicherheitslücken bei Signiervorgängen von auf einem Gerät zur Datenverarbeitung gespeicherten Daten zu beheben.

Diese Aufgabe wird mittels eines eingangs erwähnten Verfahrens dadurch gelöst, dass erfindungsgemäß

- a) zu signierende Daten über die Schnittstelle von dem Gerät an das Lesegerät übermittelt werden,
- b) in dem Lesegerät eine Prüfsumme über die übertragenen Daten gebildet wird,
- c) die Übereinstimmung der auf das Lesegerät übertragenen Daten mit den zu signierenden Daten an Hand spezifischer Merkmale der Daten überprüft wird, und
- d) bei einem Übereinstimmen der Daten eine in dem Lesegerät aus der Prüfsumme über die übertragenden Daten unter Verwendung des auf dem Speichermedium abgespeicherten Signierungsschlüssels erzeugte digitale Signatur über die Schnittstelle an das Gerät zur Verarbeitung von Daten übertragen wird, wo die Daten mit der Signatur versehen werden

Vom Gesetzgeber ist beispielsweise nach dem deutschen bzw. österreichischen Signaturgesetz vorgesehen, dass eine digitale Signatur nur dann Gültigkeit besitzt, wenn der Benutzer auch sicher sein kann, dass er bei dem Signierungsvorgang tatsächlich die von ihm ausgewählten Daten und nicht zwischen dem Auswahl- und dem Signierungsprozess veränderte Daten signiert. Allerdings ist grundsätzlich eine völlig sichere Übertragung von Daten zwischen einem Gerät zur Datenverarbeitung, wie beispielsweise einem Computer, und dem Lesegerät nicht möglich. Mit Hilfe der Erfindung wird nun eine Signaturerstellung bzw. die Übermittlung einer bereits erstellten Signatur an das Gerät zur Datenverarbeitung nur dann möglich, wenn in Folge einer vorher stattfindenden Überprüfung das Übereinstimmen der zu signierenden Daten mit den an das Lesegerät übertragenen Daten verifiziert wurde. Die Überprüfung erfolgt dabei entsprechend der Erfindung an Hand spezifischer Merkmale der Daten, beispielsweise an Hand der Daten selbst. Bei einem Nichtübereinstimmen der Daten kann der Signierungsvorgang nicht fortgesetzt werden und muss, falls gewünscht, Neubegonnen werden.

Besonders einfach lässt sich die Erfindung realisieren, wenn von dem Gerät zur Verarbeitung von Daten über die zu signierenden Daten eine Prüfsumme gebildet und die Übereinstimmung der zu signierenden mit den übertragenen Daten mittels eines Vergleichs der von dem Lesegerät und dem Gerät gebildeten Prüfsummen ermittelt wird. Als spezifische Merkmale der Daten zur Überprüfung der Übereinstimmung werden somit die unabhängig von dem Lesegerät und dem Gerät zur Datenverarbeitung gebildeten Prüfsummen verwendet.

Bei einer ersten Ausgestaltung der erfindungsgemäßen Verfahrens wird die digitale Signatur erst bei einem Übereinstimmen der Daten erzeugt und anschließend über die Schnittstelle an das Gerät zur Verarbeitung von Daten übertragen wird, während bei einer zweiten Ausführungsform die digitale Signatur nach Bildung der Prüfsumme aus dieser erzeugt wird, und nur bei einem Übereinstimmen der Daten an das Gerät zur Verarbeitung von Daten übermittelt wird

Bei einer vorteilhaften Ausführungsform der Erfindung wird die Prüfsumme mittels eines Hash-Verfahrens von dem Gerät bzw. dem Lesegerät gebildet.

Damit nicht beliebige Personen sondern nur die dazu Berechtigte mit einem Signierungsschlüssel eine digitale Unterschrift erzeugen kann, ist es günstig, wenn vor Erzeugung der Signatur die Eingabe eines dem Speichermedium für den Signierungsschlüssel zugeordneten Codes verlangt wird, und die Signatur nur bei Übereinstimmung des eingegebenen Codes mit dem dem Speichermedium zugeordneten Code erzeugt wird.

Das Speichermedium, etwa eine Chipkarte, mit dem Signierungsschlüssel befindet sich beispielsweise in einer Aufnahme des Lesegerätes, und der Code wird in der Regel mittels der Tatstatur des angeschlossenen Computers eingegeben. Bei dieser Vorgangsweise ist es allerdings mit geeigneter Soft- und/oder Hardware leicht möglich, den Code an verschiedenen Stelle auszulesen. Bei der Erfindung wird dies dadurch vermieden, dass für die Codeeingabe eine Eingabe des Lesegerätes verwendet wird. Damit verlässt der Code das Lesegerät nicht, und es bieten sich daher keine Angriffspunkte für das Auslesen des Codes.

Auf besonders einfache und trotzdem sichere Weise erfolgt die Signierung, wenn die Überprüfung und gegebenenfalls Bestätigung der Übereinstimmung der Daten von einem Benutzer durchgeführt wird, und zwar insbesondere von dem Benutzer, der den Signierungsvorgang durchführt.

Für den Benutzer ist es besonders einfach, wenn zur Überprüfung spezifische Merkmale der zu signierenden Daten an einer Ausgabe des Gerätes zur Datenverarbeitung und spezifische Merkmale der übertragenen Daten an einer Ausgabe des Lesegerätes ausgegeben werden. Insbesondere wird auf diese Weise auch das subjektive Sicherheitsgefühl des Benutzers erhöht, da dieser selbst die Übereinstimmung der Prüfsummen bestätigen kann und sich nicht auf Maschinen verlassen muss, und erst durch seine Bestätigung die endgültige Erzeugung der Signatur initiiert wird.

In diesem Zusammenhang ist es auch von Vorteil, wenn eine Bestätigung der Übereinstimmung mittels einer Eingabe des Lesegerätes durchgeführt wird.

Weiters wird die Sicherheit des Verfahrens noch dadurch erhöht, dass Zusatzinformationen betreffend die zu signierenden Daten von dem Gerät an das Lesegerät übertragen werden, wo sie an der Ausgabe des Lesegerätes ausgegeben werden, wobei die Zusatzinformationen zumindest enthalten den Namen, die Länge sowie das Erstellungsdatum der Daten. Weiters sind noch die Zusatzinformationen der zu signierenden Daten an einer Ausgabe des Gerätes zur Datenverarbeitung, etwa dem Monitor eines Computers, angezeigt. Der Benutzer kann damit auf einfache Weise auch diese Zusatzinformationen miteinander vergleichen, und nur bei einer Übereinstimmung tätigt er eine entsprechende Eingabe, die schließlich die Erstellung der digitalen Signatur durch das Lesegerät erlaubt. Bei einem Nichtübereinstimmen der Informationen hingegen wird der Benutzer die Übereinstimmung nicht Bejahen, und der Signierungsvorgang wird abgebrochen.

Nachdem die digitale Signatur erstellt und die zu signierende Datei damit versehen wurde, ist es schließlich noch zweckmäßig, wenn die mit der digitalen Signatur versehenen Daten nochmals mit den ursprünglich zu signierenden Daten verglichen werden.

Vorteilhaft ist es dabei, wenn der Vergleich von einem Benutzer unter Verwendung des Gerätes zur Verarbeitung von Daten durchgeführt wird, beispielsweise mit einem vom jeweiligen Datentyp abhängigen, zur Anzeige eingerichteten, am Gerät zur Datenverarbeitung ablaufenden Programm, wie etwa einem Textverarbeitungsprogramm.

Alternativ oder zusätzlich kann aber auch vorgesehen sein, dass der Vergleich mittels Prüfsummenbildung durchgeführt wird.

Bei der Verwendung von Lesegeräten mit relativ geringem Datenspeicher ist es günstig bzw. notwendig, wenn die zu signierenden Daten blockweise von dem Gerät an das Lesegerät übertragen und in einem Speicher zumindest zwischengespeichert werden.

An Hand der spezifischen Merkmale der jeweils übertragenen Blöcke wird ein Vergleich mit den zu signierenden Daten durchgeführt, und außerdem wird an Hand der jeweils übertragenen Blöcke auch die Prüfsummenbildung durchgeführt.

Nach einer Verwendung wird der jeweilige Block wieder aus dem Speicher gelöscht.

Zur Verwendung bei dem erfindungsgemäßen Verfahren ist insbesondere ein eingangs erwähntes Lesegerät von Vorteil, welches gemäß der Erfindung dazu eingerichtet ist, über die Schnittstelle Daten von dem Gerät zu empfangen, diese in dem Speicher zumindest zwischenzuspeichern, über die übertragenen Daten eine Prüfsumme zu bilden, und an Hand der gebildeten Prüfsumme unter Verwendung eines auf einem Speichermedium gespeicherten, mittels der Leseeinrichtung auslesbaren Signierungsschlüssels eine digitale Signatur zu erstellen und diese über die Schnittstelle an das Gerät zu übertragen.

Infolge des oftmals relativ geringen Speichers des Lesegerätes ist es günstig, wenn es dazu eingerichtet ist, die Daten blockweise zu empfangen und die empfangenen Blöcke in dem Speicher zumindest zwischenzuspeichern.

Um dem Signaturgesetz zu genügen, ist bei einer erprobten Ausführungsform das Lesegerät dazu eingerichtet, die digitale Signatur nur bei einer Übereinstimmung der zu signierenden und der übertragenen Daten zu erzeugen und an das Gerät zu übertragen bzw. erst nach einer positiven Übereinstimmung die bereits erzeugte digitale Signatur über die Schnittstelle an das Gerät zu übermitteln.

Um die Überprüfung der Übereinstimmung durch einen Benutzer zu erlauben, ist das Lesegerät dazu eingerichtet, spezifische Merkmale der übertragenen Daten an der Ausgabe auszugeben. Auf diese Weise kann der Benutzer einen Vergleich dieser Merkmale, etwa die Prüfsummen oder die Daten selbst, mit den auf einer Anzeige des Gerätes zur Datenverarbeitung angezeigten Merkmalen durchführen.

Weiters ist das Lesegerät dazu eingerichtet ist, eine Bestätigung der Übereinstimmung der Daten über eine Eingabe entgegenzunehmen.

Um wiederum dem Signaturgesetz zu genügen, ist bei einer vorteilhaften Ausführungsform das Lesegerät dazu eingerichtet, die digitale Signatur erst nach der Eingabe eines dem Speichermedium zugeordneten Codes zu erzeugen. Ohne diese Authentifizierung des Benutzers gegenüber dem Speichermedium, etwa seiner Chipkarte, ist eine Erzeugung der Signatur nicht möglich, sodass für unbefugte Personen die Erstellung einer digitalen Signatur nicht oder nur schwer möglich ist.

Damit der Code nicht mittels Hard- oder Software ausgelesen werden kann, ist vorgesehen, das die Eingabe des Codes mittels der Eingabeeinrichtung des Lesegerätes erfolgt. Auf diese Weise muss der Code nicht von einer anderen Einrichtung zu dem Lesegerät übertragen

werden, und der Code verlässt auch das Lesegerät nicht, sodass es nicht möglich ist, etwa mit dem angeschlossenen Gerät zur Datenverarbeitung den Code auszulesen.

Um eine besonders einfache Überprüfung der Übereinstimmung der zu signierenden Daten mit den an das Lesegerät übertragenen Daten zu erlauben, ist das Lesegerät dazu eingerichtet, die über die Daten gebildete Prüfsumme an der Ausgabe auszugeben. Diese Prüfsumme kann dann mit einer unabhängig davon von dem Gerät zur Datenverarbeitung über die zu signierenden Daten gebildeten Prüfsumme, die dieses an einer eigenen Ausgabe anzeigt, verglichen werden, und bei einem Übereinstimmen der Prüfsummen sind auch die zu signierenden und übertragenen Daten identisch.

Im folgenden ist die Erfindung an Hand der Zeichnung näher erläutert. In dieser zeigen

Fig. 1 eine beispielhafte schematische Darstellung einer für die Durchführung des erfindungsgemäßen Verfahrens notwendigen Hardware,

Fig. 2 eine schematische Ansicht eines erfindungsgemäßen Lesegerätes,

Fig. 3 schematisch den grundsätzlichen elektronischen Aufbau des erfindungsgemäßen Lesegerätes, und

Fig. 4 ein beispielhaftes schematisches Ablaufdiagramm des erfindungsgemäßen Verfahrens.

In der Fig. 1 ist die Hardware zur Durchführung des erfindungsgemäßen Verfahrens dargestellt. Diese besteht aus einem Gerät zur Verarbeitung von Daten COM, insbesondere einem Computer, der üblicherweise eine Ausgabe ANC, beispielsweise in Form eines Monitors aufweist. Prinzipiell kann es sich hier um einen beliebigen Rechner handeln, etwa in Form eines herkömmlichen Desktop-Computers, Notebooks, Palmtops, etc. Auch hinsichtlich des verwendeten Betriebssystems unterliegt die Erfindung grundsätzlich keinen Einschränkungen. Die Erfindung wird der einfacheren Darstellung wegen im folgenden unter Verwendung eines Computers COM dargestellt. Grundsätzlich können aber beliebige Geräte zur Verarbeitung von Daten, insbesondere auch Mobilfunkgeräte, etwa basierend auf dem GSM- oder UMTS-Standard, im Rahmen der Erfindung verwendet werden, wenn diese hardware- und softwareseitig die entsprechenden Einrichtungen zur Durchführung des erfindungsgemäßen Verfahrens aufweisen.

An den Computer COM ist mittels einer Schnittstelle SCH, beispielsweise einer seriellen Schnittstelle oder einer USB-Schnittstelle („Universal Serial Bus“) ein Lesegerät LEG anbindbar. Auch die Anbindung über eine Funkschnittstelle ist in diesem Zusammenhang vorstellbar, etwa basierend auf dem Bluetooth-Standard. Das Lesegerät LEG ist dazu eingerichtet, auf einem Speichermedium abgespeicherte Informationen auszulesen. Im Zusammenhang mit dieser Erfindung handelt es sich bei diesen Informationen insbesondere um einen Signierungsschlüssel, den sogenannten privaten Schlüssel, der auf diesem Speichermedium abgespeichert ist und der im Rahmen eines Signierungsvorganges von Dateien oder Daten zur Erzeugung einer digitalen Signatur herangezogen wird. Als Speichermedium wird in der Regel eine Chipkarte verwendet, die mit einem PIN-Code versehen ist. Bei Verwendung der Chipkarte ist eine Authentifizierung des Benutzers gegenüber der Chipkarte durch Eingabe dieses PIN-Codes notwendig.

Das österreichische und deutsche Signaturgesetz sehen nun vor, dass ein Benutzer bei der Signierung von beispielsweise einem Dokument sicher sein muss, dass er auch tatsächlich das ausgewählte Dokument signiert und dass dieses nicht in der Zeitspanne zwischen dem Auswählen und Signieren bereits verändert wird. Dies kann bei den bisher verwendeten Systemen, bei welchen an einen Computer ein Kartenlesegerät für Chipkarten angeschlossen ist, nicht gewährleistet werden. Bei diesen bekannten Systemen wird nach dem Auswählen einer Datei, die auf dem Computer gespeichert ist, sowie dem Anwählen eines entsprechenden Menüpunktes zum Erstellen der digitalen Signatur von dem Benutzer die Eingabe des PIN-Codes für beispielsweise in eine Aufnahme des Lesegerätes eingesteckte Chipkarte verlangt. Diesen Code gibt der Benutzer über eine Tastatur des Computers ein und der Code wird an das Lesegerät übertragen.

Allerdings kann eine sichere Übertragung des PIN-Codes von der Tastatur bzw. dem Computer zu dem Lesegerät nicht gewährleistet werden, da es mit geeigneter Software möglich ist, den eingegebenen PIN-Code auf dem Computer auszulesen und dann unter Umständen missbräuchlich zu verwenden.

Wird der richtige Code eingegeben, so wird der private Schlüssel von der Chipkarte an den Computer übermittelt und dort wird die Signatur für die Datei erstellt. Allerdings kann hier nicht garantiert werden, dass die zu signierende Datei nicht in der Zwischenzeit Änderungen unterworfen wurde, so dass solche Systeme einer Verwendung entsprechend dem Signaturgesetz in Österreich oder Deutschland nicht genügen.

Mit dem erfindungsgemäßen Verfahren können diese Nachteile auf einfache und kostengünstig zu realisierende Weise behoben werden. Das mit dem Computer COM über die

Schnittstelle SCH verbundene, erfindungsgemäße Lesegerät LEG, das in den Fig. 2 und Fig. 3 näher dargestellt ist, verfügt über eine Leseeinrichtung LEE zum Auslesen von auf einem Speichermedium, wie einer Chipkarte, abgespeicherten Informationen. Dazu ist beispielsweise eine Aufnahme AUF vorgesehen, in welche die Chipkarte eingesteckt werden kann. Weiters verfügt das Lesegerät LEG über einen Prozessor CPU sowie einen Speicher SPE. Der Speicher besteht dabei üblicherweise aus einem Programmspeicher SSP, bei dem es sich zumeist um einen ROM-Speicher („Read-Only Memory“) handelt, sowie aus einem Datenspeicher, der als RAM-Speicher („Random Access Memory“) und/oder einen ROM-Speicher ausgebildet sein kann.

Ein Signierungsvorgang läuft nun entsprechend der Erfindung beispielsweise wie in Fig. 4 skizziert ab. Mit dem Computer COM werden Daten, welche beispielsweise in Form einer Datei DAT auf dem Computer oder auf einem dem Computer zugeordneten Speichermedium gespeichert sind, und die der Benutzer mit seiner digitalen Unterschrift versehen möchte, ausgewählt. Diese Datei DAT wird von dem Computer auf das Lesegerät übertragen (1), welches eine Prüfsumme SUM über die übertragenen Datei bildet (4). Falls der Datenspeicher des Lesegerätes zu gering ist, um die gesamte Datei zwischenzuspeichern, wird die Datei beispielsweise blockweise übertragen, und jene Speicherbereiche der Datei, welche bereits zur Prüfsummenbildung herangezogen wurden, werden wieder aus dem Datenspeicher gelöscht. Bei der Verwendung von Lesegeräten mit ausreichender Speichergröße hingegen kann/können die Datei/Daten auch vollständig, d. h. in einem Block, an das Lesegerät übertragen werden. Auch von Seiten des Computers wird über die zu signierende Datei die Prüfsumme SUM gebildet (3), und anschließend werden die von Lesegerät und Computer gebildeten Prüfsummen miteinander verglichen (7). Für den Fall, dass die gebildeten Prüfsummen nicht übereinstimmen (8), führt dies zum Abbruch des Signiervorganges. Stimmen hingegen die beiden Prüfsummen überein (10), so wird der Benutzer zur Eingabe des PIN-Codes seiner Chipkarte, die beispielsweise in eine Aufnahme AUF des Lesegerätes LEG eingeführt wird oder ist, aufgefordert.

Bei einer vorteilhaften Ausführungsform der Erfindung wird die Überprüfung der Prüfsummen SUM durch den Benutzer durchgeführt, wozu einerseits die von dem Computer gebildete Prüfsumme an der Anzeige ANC des Computers und die von dem Lesegerät gebildete Prüfsumme an einer Anzeige ANL des Lesegerätes LEG ausgegeben wird. Hat sich der Benutzer von der Übereinstimmung der beiden Prüfsummen überzeugt, so kann er dies beispielsweise mittels einer Eingabe EIL des Lesegerätes LEG bestätigen, und er wird dann zur Eingabe des PIN-Codes aufgefordert.

Die oben genannten Maßnahmen betreffend die Überprüfung der Prüfsummen hat zum Zweck, dass der Benutzer sicher sein kann, auch jene Datei, die er zum Signieren gewählt hat, tatsächlich zu signieren, und nicht eine in der Zwischenzeit veränderte. Um dahingehend die Sicherheit, insbesondere das subjektive Sicherheitsempfinden des Benutzers, noch zu erhöhen, kann auch noch vorgesehen sein, dass von dem Computer Zusatzinformationen INF betreffend die zu signierende Datei an das Lesegerät übertragen werden (2). Diese Zusatzinformationen, die dann beispielsweise einerseits an der Anzeige ANC des Computers und andererseits an der Anzeige des Lesegerätes ANL ausgegeben werden, können von dem Benutzer miteinander verglichen werden (5) und die Übereinstimmung kann beispielsweise mit der Eingabe EIL des Lesegerätes bestätigt werden. Sollten die Zusatzinformationen, die zumindest den Namen, die Länge und das Erstellungsdatum der Datei enthalten, nicht übereinstimmen (6), so führt dies zum Abbruch des Signierungsvorganges.

Bei Übereinstimmung (9) der am Computer sowie am Lesegerät angezeigten Zusatzinformation INF sowie der Übereinstimmung der Prüfsummen (10) wird der Benutzer zur Eingabe seines PIN-Codes aufgefordert. Erfolgt hierbei eine falsche Eingabe des Codes (11) so führt dies entweder zum Abbruch des Vorgangs (12) oder zu einer neuerlichen Aufforderung (13) an den Benutzer, den Code einzugeben.

Bei Vorliegen des richtigen Codes (14) wird die digitale Signatur SIGN erstellt (15) und an den Computer übermittelt (16). Von diesem wird dann die zu signierende Datei mit der Signatur SIGN versehen (17):

Auf diese Weise entsteht eine neue Datei, welche neben der ursprünglichen Datei auch noch die digitale Signatur enthält. Außerdem kann diese Datei auch noch ein Zertifikat, welches ebenfalls von der Chipkarte über das Lesegerät an den Computer übermittelt wurde, enthalten. An Hand dieses Zertifikats kann ein Empfänger der digital signierten Datei eindeutig den öffentlichen Schlüssel und somit die digitale Signatur einer bestimmten Person zuordnen. Die Übermittlung des Zertifikats von dem Lesegerät an das Gerät zur Datenverarbeitung ist allerdings nicht zwingend notwendig. Beispielsweise kann dieses Zertifikat auch von einer geeigneten Stelle, etwa einem Server im Internet, von einem Empfänger einer digital signierten Datei heruntergeladen werden („Trust-Center“).

Wie an Hand des obigen Ausführungsbeispiels dargestellt, können mit dem erfindungsgemäßen Verfahren auf einfache Weise Daten oder Dateien, die auf einem Gerät zur Datenverarbeitung oder auf einem diesem zugeordneten Speicher abgelegt sind, mit einer digitalen Signatur versehen werden. Der zeitliche Ablauf der Schritte (1) - (8) des Verfahrens muss natürlich nicht genau dem oben geschilderten entsprechen. Es ist durchaus beispielsweise

auch denkbar, dass vorerst von der ausgewählten Datei von dem Computer eine Prüfsumme gebildet wird (3) und erst anschließend die Datei an das Lesegerät übermittelt wird (1). Eine Änderung des zeitlichen Ablaufs der oben beschriebenen Schritte führt daher nicht aus dem Schutzzumfang der Ansprüche heraus.

Das Verfahren wurde mittels einer vorteilhaften Ausführungsform der Erfindung, bei der die über die übertragenen und zu signierenden Daten gebildeten Prüfsummen durch einen Benutzer miteinander verglichen werden, erläutert. Möglich ist aber auch, dass etwa der Vergleich nicht von einem Benutzer sondern von dem dazu eingerichteten Computer oder Lesegerät durchgeführt wird.

Außerdem ist entsprechend dem Schutzbegehren nicht zwingend ein Vergleich der übertragenen Daten mit den zu signierenden Daten an Hand der Prüfsummen notwendig. Die Verwendung von Prüfsummen als spezifisches Merkmal der Daten ist vor allem aus dem Grund vorteilhaft, dass diese auf den zumeist nur kleinen Anzeigen eines Lesegerätes problemlos angezeigt werden können. Grundsätzlich kann der Vergleich der Daten aber auch unter Verwendung anderer spezifischer Merkmale durchgeführt werden, beispielsweise kann der Vergleich unmittelbar an Hand der Datei/den Daten erfolgen, indem die zu signierende Datei, etwa ein mit einem Textverarbeitungsprogramm verfasstes Dokument, an dem Monitor des Computers, und die übertragene Datei an einer dazu geeigneten Anzeige des Lesegerätes ausgegeben und die angezeigten Dateien von dem Benutzer miteinander verglichen werden.

Nochmals zurückkommend auf die mehrmals angesprochenen Prüfsummen sei hier noch angemerkt, dass diese vorteilhafterweise mittels des einem Fachmann bekannten Hash-Verfahrens gebildet werden, insbesondere da dies in den derzeitigen Fassungen des deutschen und österreichischen Signaturgesetzes vorgesehen ist. Allerdings ist prinzipiell die Prüfsummenbildung nicht auf dieses Verfahren eingeschränkt, auch andere Verfahren sind durchaus denkbar.

Die digitale Signatur entsteht nun aus der Verschlüsselung der von dem Lesegerät gebildeten Prüfsumme mit dem privaten, geheimen, auf der Chipkarte gespeicherten Signierungsschlüssel. Die so gebildete digitale Signatur wird dann zumeist gemeinsam mit dem ebenfalls auf der Chipkarte gespeicherten Zertifikat, welches unter anderem den öffentlichen Schlüssel zur Entschlüsselung enthält und somit zur Überprüfen der Authentikation und Integrität dient, an den Computer übertragen, wo die zu signierende Datei damit versehen wird.

Nachdem die Datei mit der Signatur und eventuell dem Zertifikat versehen worden ist, kann sie von dem Benutzer nochmals überprüft werden. Beispielsweise wird dazu ein Anzeigeprogramm verwendet, etwa ein Textverarbeitungsprogramm für Textdateien. Es kann aber auch vorgesehen sein, dass diese Überprüfung nochmals an Hand spezifischer Merkmale, wie etwa einer Prüfsumme, durchgeführt wird.

PATENTANSPRÜCHE

1. Verfahren zur Erzeugung digitaler Signaturen für Daten, welche auf einem Gerät (COM) zur Verarbeitung von Daten oder einem dem Gerät zugeordneten Speicher gespeichert sind, unter Verwendung eines auf einem physikalisch von dem Gerät oder dem Speicher getrennten Speichermedium gespeicherten Signierungsschlüssels, welcher mittels eines an das Gerät (COM) über eine Schnittstelle (SCH) anbindbaren Lesegerätes (LEG) von dem Speichermedium zur Erzeugung einer digitalen Signatur auslesbar ist,

dadurch gekennzeichnet, dass

a) zu signierende Daten über die Schnittstelle (SCH) von dem Gerät (COM) an das Lesegerät (LEG) übermittelt werden,

b) in dem Lesegerät (LEG) eine Prüfsumme über die übertragenen Daten gebildet wird,

c) die Übereinstimmung der auf das Lesegerät (LEG) übertragenen Daten mit den zu signierenden Daten an Hand spezifischer Merkmale der Daten überprüft wird, und

d) bei einem Übereinstimmen der Daten eine in dem Lesegerät aus der Prüfsumme über die übertragenden Daten unter Verwendung des auf dem Speichermedium abgespeicherten Signierungsschlüssels erzeugte digitale Signatur über die Schnittstelle (SCH) an das Gerät (COM) zur Verarbeitung von Daten übertragen wird, wo die Daten mit der Signatur versehen werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass von dem Gerät (COM) zur Verarbeitung von Daten über die zu signierenden Daten eine Prüfsumme gebildet und die Übereinstimmung der zu signierenden mit den übertragenen Daten mittels eines Vergleichs der von dem Lesegerät (LEG) und dem Gerät (COM) gebildeten Prüfsummen ermittelt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die digitale Signatur erst bei einem Übereinstimmen der Daten erzeugt und anschließend über die Schnittstelle (SCH) an das Gerät (COM) zur Verarbeitung von Daten übertragen wird.

4. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die digitale Signatur nach Bildung der Prüfsumme aus dieser erzeugt wird, und nur bei einem Übereinstimmen der Daten an das Gerät (COM) zur Verarbeitung von Daten übermittelt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Prüfsumme mittels eines Hash-Verfahrens von dem Gerät (COM) bzw. dem Lesegerät (LEG) gebildet wird.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass vor Erzeugung der Signatur die Eingabe eines dem Speichermedium für den Signierungsschlüssel zugeordneten Codes verlangt wird, und die Signatur nur bei Übereinstimmung des eingegebenen Codes mit dem dem Speichermedium zugeordneten Code erzeugt wird.
7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass für die Codeeingabe eine Eingabe (EIL) des Lesegerätes (LEG) verwendet wird.
8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Überprüfung und gegebenenfalls Bestätigung der Übereinstimmung der Daten von einem Benutzer durchgeführt wird.
9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass zur Überprüfung spezifische Merkmale der zu signierenden Daten an einer Ausgabe (ANC) des Gerätes (COM) zur Datenverarbeitung und spezifische Merkmale der übertragenen Daten an einer Ausgabe (ANL) des Lesegerätes (LEG) ausgegeben werden.
10. Verfahren nach Anspruch 8 oder 9, dadurch gekennzeichnet, dass eine Bestätigung der Übereinstimmung mittels einer Eingabe (EIL) des Lesegerätes (LEG) durchgeführt wird.
11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass Zusatzinformationen betreffend die zu signierenden Daten von dem Gerät (COM) an das Lesegerät (LEG) übertragen werden, wo sie an der Ausgabe (ANL) des Lesegerätes (LEG) ausgegeben werden.
12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass die Zusatzinformationen zumindest enthalten den Namen, die Länge sowie das Erstellungsdatum der Daten.
13. Verfahren nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass die mit der digitalen Signatur versehenen Daten nochmals mit den ursprünglich zu signierenden Daten verglichen werden.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass der Vergleich von einem Benutzer unter Verwendung des Gerätes (COM) zur Verarbeitung von Daten durchgeführt wird.
15. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass der Vergleich mittels Prüfsummenbildung durchgeführt wird.
16. Verfahren nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass die zu signierenden Daten blockweise von dem Gerät (COM) an das Lesegerät (LEG) übertragen und in einem Speicher (SPE) zumindest zwischengespeichert werden.
17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass an Hand spezifischer Merkmale der jeweils übertragenen Blöcke ein Vergleich mit den zu signierenden Daten durchgeführt wird.
18. Verfahren nach Anspruch 16 oder 17, dadurch gekennzeichnet, dass an Hand der jeweils übertragenen Blöcke die Prüfsummenbildung durchgeführt wird.
19. Verfahren nach Anspruch einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, dass nach einer Verwendung der jeweilige Block aus dem Speicher (SPE) gelöscht wird.
20. Lesegerät für Speichermedien, welches über zumindest eine Schnittstelle (SCH) mit Geräten (COM) zur Datenverarbeitung verbindbar ist, mit einer Leseeinrichtung (LEE), zumindest einem Prozessor (CPU), zumindest einer Speichereinrichtung (SPE), zumindest einer Ausgabe (ANL) und zumindest einer Eingabe (EIL), dadurch gekennzeichnet, dass es dazu eingerichtet ist, über die Schnittstelle (SCH) Daten von dem Gerät (COM) zu empfangen, diese in dem Speicher (SPE) zumindest zwischenzuspeichern, über die übertragenen Daten eine Prüfsumme zu bilden, und an Hand der gebildeten Prüfsumme unter Verwendung eines auf einem Speichermedium gespeicherten, mittels der Leseeinrichtung (LEE) auslesbaren Signierungsschlüssels eine digitale Signatur zu erstellen und diese über die Schnittstelle (SCH) an das Gerät (COM) zu übertragen.
21. Lesegerät nach Anspruch 20, dadurch gekennzeichnet, dass es dazu eingerichtet ist, die Daten blockweise zu empfangen und die empfangenen Blöcke in dem Speicher (SPE) zumindest zwischenzuspeichern.
22. Lesegerät nach Anspruch 20 oder 21, dadurch gekennzeichnet, dass es dazu eingerichtet ist, die digitale Signatur nur bei einer Übereinstimmung der zu signierenden und der

übertragenen Daten zu erzeugen und an das Gerät (COM) zu übertragen bzw. erst nach einer positiven Übereinstimmung die bereits erzeugte digitale Signatur über die Schnittstelle (SCH) an das Gerät (COM) zu übermitteln.

23. Lesegerät nach einem der Ansprüche 20 bis 22, dadurch gekennzeichnet, dass es dazu eingerichtet ist, spezifische Merkmale der übertragenen Daten an der Ausgabe (ANL) auszugeben.

24. Lesegerät nach einem der Ansprüche 20 bis 23, dadurch gekennzeichnet, dass es dazu eingerichtet ist, eine Bestätigung der Übereinstimmung der Daten über eine Eingabe (EIL) entgegenzunehmen.

25. Lesegerät nach einem der Ansprüche 20 bis 24, dadurch gekennzeichnet, dass es dazu eingerichtet ist, die digitale Signatur erst nach der Eingabe eines dem Speichermedium zugeordneten Codes zu erzeugen.

26. Lesegerät nach Anspruch 25, dadurch gekennzeichnet, dass die Eingabe des Codes mittels der Eingabe (EIL) des Lesegerätes (LEG) erfolgt.

27. Lesegerät nach einem der Ansprüche 20 bis 26, dadurch gekennzeichnet, dass es dazu eingerichtet ist, die über die Daten gebildete Prüfsumme an der Ausgabe (ANL) auszugeben.

1/2

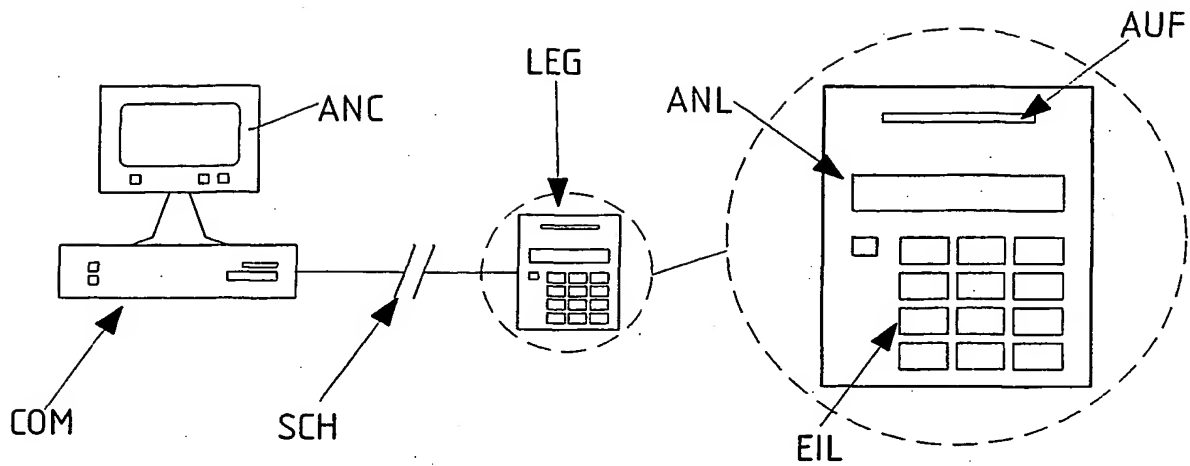


Fig. 1

Fig. 2

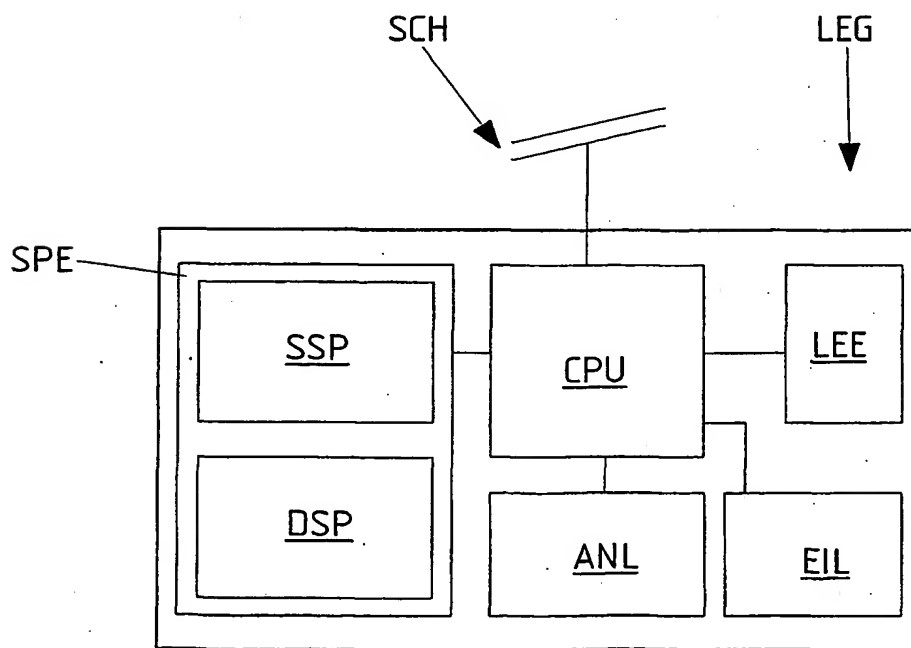


Fig. 3

2/2

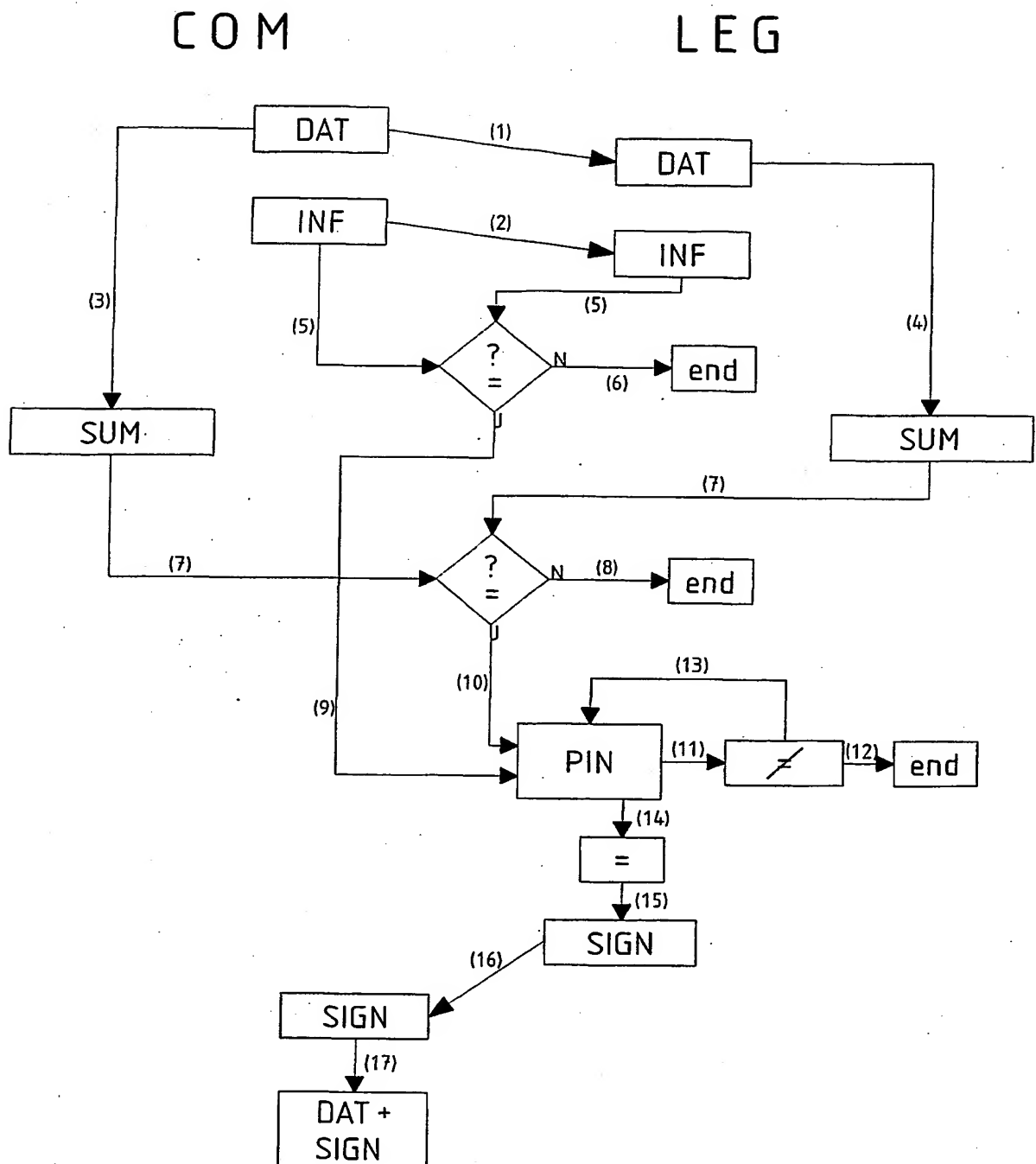


Fig. 4